Deutscher Bundestag **Drucksache 19/1328**

19. Wahlperiode 21.03.2018

Antrag

der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Kerstin Andreae, Dr. Danyal Bayaz, Franziska Brantner, Agnieszka Brugger, Dr. Anna Christmann, Kai Gehring, Stefan Gelbhaar, Erhard Grundl, Ottmar von Holz, Dieter Janecek, Katja Keul, Sven-Christian Kindler, Dr. Gerhard Schick, Maria Klein-Schmeink ,Christian Kühn, Renate Künast, Dr. Tobias Lindner, Claudia Müller, Beate Müller-Gemmeke, Corinna Rüffer, Manuel Sarrazin, Frithjof Schmidt, Stefan Schmidt, Kordula Schulz-Asche, Margit Stumpp und der Fraktion BÜNDNIS 90/DIE GRÜNEN

IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die Stärkung der IT-Sicherheit ist eine zentrale Bedingung für das Gelingen der gesellschaftlichen Gestaltung der Digitalisierung, für die Schaffung von Vertrauen in digitale Angebote und Infrastrukturen, für den Erhalt von Freiheit sowie für die Sicherung von Frieden.

Der jüngst bekannt gewordene IT-Angriff auf das deutsche Regierungsnetz, eines der bestgeschützten Netze der Bundesrepublik, steht in einer ganzen Reihe von Angriffen auf IT-Systeme und digitale Infrastrukturen bundes-, europa- und weltweit. Er hat die Verletzlichkeit von IT-Systemen und digitalen Infrastrukturen in einer zunehmend vernetzten Welt erneut schmerzlich vor Augen geführt.

Gleichzeitig hat der Angriff erneut die Notwendigkeit aufgezeigt, dringend erforderliche Schritte zur Verbesserung der IT-Sicherheit zu unternehmen. Die bisherige IT-Sicherheitspolitik der Bundesregierung ist bislang von zahlreichen Widersprüchen gekennzeichnet und insgesamt kritisch zu hinterfragen.

Die bisherige Politik der Bundesregierung ohne ganzheitlichen und konsequenten IT-Schutz hat maßgeblich dazu geführt, dass das Vertrauen in digitale Infrastrukturen und E-Government-Angebote in den vergangenen Jahren gravierend gelitten hat und zahlreiche öffentliche IT-Großprojekt in der Vergangenheit an massiven Akzeptanzproblemen gescheitert sind.

Die Bedeutung einer guten IT-Sicherheit nimmt auch durch die rasante Entwicklung und Verbreitung des „Internet der Dinge“ und der weiteren Zunahme von vernetzten Geräten rasant zu. Ohne Verbrauchervertrauen steht die Digitalisierung auch im Privatbereich auf dem Spiel.

Statt ihrer Schutzpflicht für die Vertraulichkeit und Integrität informationstechnischer Systeme und dem Grundrecht auf Privatheit der Kommunikation nachzukommen, stellt das Agieren der Bundesregierung selbst eine Gefahr für die IT-Sicherheit in Deutschland dar.

Exemplarisch genannt seien die Einrichtung einer rechtlich unregulierten „Zentralen Stelle für Informationstechnik im Sicherheitsbereich“ (ZITIS), mit der der Staat zum Hacker verschlüsselter Kommunikation wird, die anhaltende Zusammenarbeit mit fragwürdigen IT-Sicherheitsfirmen sowie der staatliche Ankauf, das bewusste Offenhalten und die Nutzung von IT-Sicherheitslücken („Zero-Day-Exploits“) für Überwachungsmaßnahmen – anstatt diese zu schließen.

Zu lange hat die Bundesregierung die im Mittelpunkt stehenden Fragen der IT-Sicherheit der Selbstregulierung der Wirtschaft überlassen und eine Politik verfolgt, die die Interessen von Sicherheitsbehörden vor den effektiven Schutz von Grundrechten und sichere digitale Angebote stellt.

Die bisherigen gesetzgeberischen Aktivitäten der Bundesregierung zum Schutz digitaler Infrastrukturen und Kommunikation sind absolut unzureichend. Zudem hat es die Bundesregierung bislang verpasst, klare Zuständigkeiten zu benennen und diejenigen stärker zu unterstützen, die proaktiv in gute IT-Sicherheitspolitik investieren. Ein ganzheitlicher Ansatz ist jedoch dringend notwendig: IT-Sicherheit und Datenschutz sind konstitutiv für die zunehmend digitale Demokratie.

Statt die seit Jahren bekannten Defizite im Bereich der IT-Sicherheit abzustellen, ist ein anhaltendes cyberpolitisches Wettrennen verschiedener bundespolitischer Akteure zu beobachten, die um digitalpolitische Kompetenzen ringen. Durch ungeklärte Zuständigkeiten und fehlende rechtliche Regelungen entstehen neue Gefahren für die IT-Sicherheit. Zu beobachten ist zudem ein inflationärer Gebrauch von Begrifflichkeiten, die häufig bewusst nicht klar definiert sind.

Einer solchen Politik des digitalen Auf- und Wettrüstens, die auch über – verfassungsrechtlich hoch umstrittene – digitalen Gegenschläge („Hack back“) und einen neuen „Cyberwar“ fantasiert, muss eine besonnene, an realen Bedrohungslagen orientierte Politik entgegengesetzt werden, die auf bestmöglich geschützte IT-Systeme, digitale Infrastrukturen sowie innovative IT-Sicherheitslösungen setzt.

Um IT-Sicherheit effektiv zu erhöhen, ist die schnellstmögliche Umsetzung eines ganzen Bündels an Maßnahmen notwendig.

II. Der Deutsche Bundestag fordert die Bundesregierung auf, zur Stärkung der IT-Sicherheit in Deutschland folgende Maßnahmen zu ergreifen:

a. IT-Sicherheit als verfassungsrechtliche Gewährleistungspflicht des Staates: Die Bundesregierung muss die Schutzpflichten aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme als oberste Priorität einer neuen IT-Sicherheitspolitik anerkennen. Infolgedessen sind Maßnahmen zum Ausbau der IT-Sicherheit zu stärken und Maßnahmen, die die IT-Sicherheit zugleich erheblich schwächen, konsequent abzulehnen.

b. IT-Sicherheit differenziert vorantreiben: Um staatliche und andere Infrastrukturen zu schützen, müssen ganzheitliche Sicherheitskonzepte vorangetrieben werden. Die Bundesregierung muss unter anderem schnellstmöglich ein neues IT-Sicherheitsgesetz vorlegen. Das Gesetz muss mehr als nur die bisher berücksichtigte kritische Infrastruktur umfassen und statt allein auf Mindeststandards und passive Meldepflichten von Unternehmen zu setzen, auch öffentliche Stellen einbeziehen. Insgesamt muss

es sehr viel stärker auf Anreize für proaktive Investitionen in gute IT-Sicherheitslösungen setzen. Auf europäischer Ebene muss sich die Bundesregierung im Rahmen der Verordnung zur Reform von ENISA und der Entwicklung eines Zertifizierungsrahmens der Sicherheit von Informations- und Kommunikationstechnik für klare und verbindliche IT-Mindeststandards einsetzen.

c. Koordination und klare Zuständigkeit: Die Verantwortung für IT-Sicherheit muss aus dem Bundesinnenministerium herausgelöst werden, um den effektiven Grundrechtsschutz zu stärken. Zudem müssen klare Zuständigkeiten innerhalb der Bundesregierung benannt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird – zumindest im Rahmen seiner Aufgaben gegenüber Wirtschaft und Zivilgesellschaf - unabhängig gestellt und in seiner Beratungsfunktion gegenüber Bürgerinnen und Bürgern wie Unternehmen gestärkt. Eine gesonderte Bund und Länder übergreifende unabhängige Institution muss für die Sicherheit des elektronischen Rechtsverkehrs einschließlich des besonderen elektronischen Anwaltspostfaches zuständig sein, um Gefahren für das Justizsystem entgegenzuwirken. Die rechtliche Grundlage und der Aufgabenzuschnitt für die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (ZITIS) sind kritisch zu überprüfen und eine grundrechtlich orientierte gesetzliche Regelung vorzulegen.

d. Zusammenarbeit im „Cyberabwehrzentrum“ (CAZ) auf rechtliche Grundlage stellen: Das sogenannte "Cyberabwehrzentrum" der Bundesbehörden braucht hinreichend bestimmte Regelungen bezüglich seiner konkreten Aufgaben und der Zusammenarbeit der beteiligten Behörden. Sowohl die Rechte und Pflichten der beteiligten Behörden als auch Maßgaben für unterschiedliche Handlungsformate und der Umgang mit Informationen und Daten müssen klar gesetzlich geregelt werden.

e. Aufsichtsstrukturen stärken: Bestehende Aufsichtsstrukturen müssen besser ausgestattet und angekündigte, neue Aufsichtsstrukturen, wie beispielsweise eine bislang nicht näher definierte „Digitalagentur“ klar von bestehenden Strukturen abgegrenzt werden. Das Personal der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) muss in einem neuen Herausforderungen und gesetzlichen Aufgaben angemessenen Umfang von circa 200 zusätzlichen Stellen aufgestockt werden. Die Bundesregierung wirkt im Zusammenspiel mit den Ländern darauf hin, dass auch die Aufsichtsbehörden auf Landesebene als Experten vor Ort eine angemessene, auch gesetzlich gebotene Stärkung erfahren.

f. Verzicht auf IT-Sicherheit gefährdende Maßnahmen: Insbesondere bei der Strafverfolgung, der Gefahrenabwehr und Gefahrenbeobachtung muss auf IT-Sicherheit gefährdende Maßnahmen verzichtet werden. Hierzu gehören unter anderem offensive Operationen und sogenannte „Hack backs“, der staatliche Ankauf, das Offenhalten und die Nutzung von bislang nicht öffentlich bekannten Sicherheitslücken („Zero-Day-Exploits“) und Überlegungen einer gesetzlichen Verpflichtung für Unternehmen, Hintertüren in Hard- und Software zu verbauen. Auch eine Militarisierung ziviler Netzwerkinfrastruktur und die Nutzung dieser als weitere Domäne der Kriegsführung sind abzulehnen und international zu ächten. Die behördliche Ausnutzung von Schwachstellen („vulnerabilities“) kann und darf nur auf hinreichend konkreter gesetzlicher Grundlage und in einem rechtsstaatskonformen Verfahren erfolgen.

g. Transparenz und Kontrolle stärken: Sicherheitslücken müssen schnellstmöglich im Zusammenspiel staatlicher und privater Akteure geschlossen

und der Öffentlichkeit bekannt gemacht werden. Die Aktivitäten der Nachrichtendienste und der Bundeswehr im digitalen Raum müssen klar und bestimmt, unter strenger Beachtung grundgesetzlicher Vorgaben, gesetzlich geregelt und effektiv und wirksam vom Parlament kontrolliert werden können. Jeglicher Einsatz von digitalen Einsatzkapazitäten der Bundeswehr muss ebenso wie der Einsatz sonstiger militärischer Kräfte der parlamentarischen Kontrolle des Deutschen Bundestages unterliegen. Über ein integriertes parlamentarisches Kontrollregime ist sicherzustellen, dass die gravierenden Probleme und Lücken bei der parlamentarischen Kontrolle von Operationen und Aktivitäten der Bundeswehr und Nachrichtendienste im digitalen Raum behoben werden und das Parlament sowie seine zuständigen Gremien umfassend, konsistent und zeitnah über entsprechende Aktivitäten unterrichtet werden.

h. Zuständigkeit für die übergreifende Beobachtung von hybriden Angriffen schaffen: Um eine an realen Bedrohungslagen orientierte IT-Sicherheitspolitik verfolgen zu können, ist für begriffliche Klarheit zu sorgen. Zur systematischen Beobachtung möglicher gezielter Angriffe, insbesondere auf zivile und für das staatliche Wohl relevante digitale Infrastrukturen und zur Erstellung eines an realen Gegebenheiten orientierten Lagebilds ist eine eindeutige ministeriell-koordinierende Zuständigkeit für „hybride Bedrohungen“ (hybrid threats) zu schaffen. Zur Bewertung einer etwaigen Zurechenbarkeit von Angriffen (Attribution) bedarf es zudem einer eigenständigen, fachlich unabhängigen Organisationseinheit.

i. Verschlüsselung von Daten und Kommunikation stärken: Bei allen E-Government-Angeboten sind beste IT-Sicherheitslösungen auf dem neuesten Stand der Technik zum Standard zu machen. Hierzu gehören unter anderem durchgehende Ende-zu-Ende-Verschlüsselungen und die verpflichtende Nutzung sicherer Hypertext-Übertragungsprotokolle. Mit einer Verschlüsselungsoffensive wird Aufbau, Betrieb und Angebot von echter Ende-zu-Ende-Verschlüsselung bei allen IT-Großprojekten gefördert. Internetzugangsprovider werden zur sicheren und verbraucherfreundlichen Verschlüsselung der Kommunikation ihrer Kundinnen und Kunden verpflichtet. Gängige Verfahren zur Verschlüsselung von E-Mails sind stärker als bislang zu unterstützen und auch in allen Bundesministerien schnellstmöglich umzusetzen.

j. Datenschutz und IT-Sicherheit zusammen denken: Überfällige gesetzgeberische Handlungen im Bereich des Datenschutzes müssen schnellstmöglich angegangen werden. Dazu zählt insbesondere die aktive politische Begleitung der E-Privacy-Verordnung. Auch für die nationale Umsetzung der EU-Datenschutzgrundverordnung bedarf es weiterer gesetzlicher Anstrengungen. Insbesondere der Schutzbedürftigkeit von Kindern und Jugendlichen muss hierbei angemessen Rechnung getragen werden. Sehr viel stärker als bislang sind innovative Datenschutzmodelle wie Datenschutz by design und by default als wichtige Bausteine einer guten digitalen Standortpolitik und als echter Wettbewerbsvorteil auf dem rasant wachsenden Markt digitaler Sicherheitslösungen sehr viel stärker als bisher zu unterstützen. Gleiches gilt für proaktive Anreize für innovative Datenschutzmodelle, beispielsweise über Auditierung und Zertifizierungsverfahren. Entsprechende Zertifizierungen für voreingestellten Datenschutz und höchste IT-Sicherheitsstandards müssen Voraussetzung öffentlicher Förderung und Beschaffung sein.

k. Offene und überprüfbare Standards stärken: Zur Verringerung riskanter, einseitiger Abhängigkeiten und zur Stärkung der IT-Sicherheit durch

Überprüfbarkeit der verwendeten Systeme ist freie, quelloffene Software als zentraler Baustein für eine sichere und zukunftsfähige IT-Landschaft sehr viel stärker zu unterstützen als bislang. So sind unter anderem die Vorgaben bei öffentlichen IT-Beschaffungen hinsichtlich der Überprüfbarkeit anzupassen und eine stärkere Kooperation zwischen Bund und Ländern über den IT-Planungsrat sicherzustellen. Bei Wahlsoftware ist die Veröffentlichung des Quellcodes zur Überprüfbarkeit sicherzustellen. Um die Qualität freier und offener Software zu verbessern, ist ein Fonds für die Prämierung der Identifizierung, Behebung und Bekanntmachung von Fehlern in quelloffener Software („Bug Bounties") zu schaffen und die Forschungsförderung in dem Bereich zu intensivieren.

l. Wirtschaft unterstützen: Die IT- und Produktsicherheit in Deutschland ist auch als wichtiges Qualitätsmerkmal im internationalen Wettbewerb zu stärken. Dabei sind mit rechtlichen Vorgaben, Anreize für Unternehmen zu schaffen, beispielsweise mit Zertifizierungen, in gute und sichere IT-Lösungen, insbesondere beim „Internet-der-Dinge" zu investieren. Dazu gehören unter anderem Mindestfristen, in denen Anbieter verpflichtet sind, zeitnahe Sicherheitsupdates zur Verfügung zu stellen. Die Umsetzung der Empfehlungen der internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation bezüglich eindeutiger Vorgaben für den Sicherheitssupport von Geräten sind zu prüfen, auch hinsichtlich der etwaigen Freigabe des eingesetzten Quellcodes im Rahmen einer Open-Source-Lizenz. Kleinere und mittlere Unternehmen müssen bei sicherheitstechnischen Herausforderungen durch ein dezentrales und unabhängiges IT-Beratungsnetzwerk unterstützt werden. Haftungsanreize für alle in der IT-Kette verantwortlichen Stellen werden gestärkt.

m. Stärkung von Haftung: Gerade hinsichtlich der Besonderheiten und Risiken vernetzter IT-Systeme müssen bestehende Haftungsregelungen überprüft und neue gesetzliche Regelungen vorgelegt werden. Ein Regelungsbedarf besteht beispielsweise bei der Haftung im Falle von Sicherheitsverletzungen wie fahrlässig implementierter oder nicht beseitigter Sicherheitslücken von Herstellern (Produktsicherheitsgesetze, Produkthaftung, Produzentenhaftung, Schutzgesetze), der Verkäufer-Haftung bei Hard- und Software (Gewährleistung, Fehlerbegriff, zugesicherte Eigenschaft, berechtigte Erwartung des Käufers) sowie von Dienstleistern (Sicherheitspflichten und berechtigte Sicherheitserwartungen der Nutzer). Zu verhindern ist, dass häufig komplex gelagerte Streitfälle von geteilter und oftmals nicht konkret feststellbarer Verantwortung von Herstellern, Diensteanbietern und Nutzerinnen und Nutzern einseitig zu Lasten der Endnutzerinnen und -nutzer ausgehen.

n. Massenüberwachung stoppen, gesetzliche Grundlagen für Telekommunikations-Überwachungsmaßnahmen reformieren: Anlasslose Massendatenspeicherungen ohne erwiesenen sicherheitspolitischen Mehrwert zu Lasten von Grundrechten müssen kritisch hinterfragt werden. Zudem sind zumindest verhältnismäßige Rechtsgrundlagen für die bereits bestehende Quellen-Telekommunikationsüberwachung und die Onlinedurchsuchung zu schaffen und die Eingriffsschwellen gesetzlich zu erhöhen. Bei den eingesetzten Programmen muss die Verfassungskonformität durch eine Quellcodeprüfung durch die Bundesbeauftragte für den Datenschutz nachgewiesen werden. Eine Überprüfung der Verfassungskonformität durch die einsetzenden Stellen selbst ist abzulehnen. Der Einsatz entsprechender Programme in einem grundrechtlich hochsensiblen Bereich durch Geheimdienste bleibt unzulässig.

o. Forschungsförderung für die IT-Sicherheit stärken: Im Bereich der IT-Sicherheit gibt es ein enormes Know-How in Deutschland. Dieses gilt es zu sichern und auszubauen. Öffentliche Forschungsaktivitäten müssen in Zusammenarbeit mit den Ländern verstetigt und intensiviert werden. Im internationalen Wettbewerb um die besten IT-Sicherheitskonzepte müssen hervorragende Expertinnen und Experten in Deutschland aus der internationalen Wissenschaftscommunity zusammengebracht werden. U.a. das Zentrum Karlsruhe Security Technology Laboratories (KASTEL), das Center for Research in Security and Privacy (CRISP) in Hessen und das Center for IT-Security, Privacy and Accountability (CISPA) in Saarbrücken sind wichtige Leuchttürme für den IT-Sicherheitsstandort Deutschland. Sie müssen dauerhaft zu wichtigen Säulen einer kohärenten Gesamtstrategie für eine anwendungsorientierte IT-Sicherheits-Forschung in Deutschland werden.

p. Fachkräftesicherung voranbringen: IT-Sicherheit braucht gut ausgebildete Fachkräfte, sei es zur Verhinderung von IT-Angriffen, sei es für die Entwicklung von Sicherheitssystemen und –strategien. Dies gilt genauso für die Wirtschaft wie für die öffentliche Hand. Gerade angesichts eines Wettkampfes um die besten Fachkräfte mit der freien Wirtschaft muss die Attraktivität der öffentlichen Hand als Arbeitsgeber ständig weiterentwickelt werden. Um dies zu gewährleisten, ist der Ausbau geeigneter Aus- und Weiterbildungsstrukturen erforderlich. Insgesamt müssen Ausbildungssysteme im IKT-Bereich möglichst praxisnah sein und IT-Sicherheitsaspekte angesichts gestiegener, sich stetig wandelnder Herausforderungen verstärkt berücksichtigen. Die Ausbildungsordnungen müssen gemeinsam mit den Sozialpartnern regelmäßig auf ihren Modernisierungsbedarf überprüft werden. Bei der Fachkräfteausbildung muss auch der bestehende Gender Gap im Bereich der Informations- und Kommunikationstechnologien entschlossen angegangen werden.

q. Verzicht auf Kooperationen mit fragwürdigen IT-Sicherheits-Firmen: Solange staatliche Stellen nicht selbst in der Lage sind, entsprechende Programme zu programmieren und deren Verfassungskonformität einwandfrei und überprüfbar sicherzustellen, ist auf eine Zusammenarbeit mit Firmen, von denen bekannt ist, dass sie mit Sicherheitslücken handeln und ihre Produkte auch an autoritäre und totalitäre Staaten veräußern - auch im Sinne der globalen IT-Sicherheit - zu verzichten. Eine weitere Effektivierung bestehender Kontrollregime muss sowohl auf bundes-, europa- als auch internationaler Ebene angestrebt werden. In diesem Kontext ist unter anderem auch die Prüfung der Einführung schwarzer Listen mit Unternehmen, die nachweislich gegen bestehende Kontrollregime verstoßen haben, zu überprüfen.

r. Sensibilisierung und Schulung von Mitarbeiterinnen und Mitarbeitern: Einer der größten Angriffsvektoren in Behörden und Unternehmen sind Mitarbeiterinnen und Mitarbeiter. Identitätsklau, gefälschte Zugangsseiten und mit Schadsoftware versehene Anhänge, „social engineering“, also Versuche der zwischenmenschlichen Beeinflussung mit dem Ziel, Informationen zu erlangen und fremde Computersysteme zu infiltrieren sind regelmäßige Instrumente für IT-Angriffe. Mitarbeiterinnen und Mitarbeiter in öffentlichen Behörden müssen flächendeckend und regelmäßig sowie zertifizierte und am Stand der Technik orientierte Sicherheitsschulungen für den Umgang mit IT-Systemen angeboten werden. Gerade für Mitarbeiterinnen und Mitarbeiter in besonders sensiblen Bereichen müssen diese Fortbildungsmaßnahmen auf konkreten Bedrohungslagen

zugeschnitten sein. Bei der Vermittlung von Medienkompetenz müssen Fragen der Daten- und IT-Sicherheit sehr viel stärker gewichtet werden als bisher. Im Zusammenspiel mit den Ländern sind entsprechende Angebote zu überprüfen und auszubauen.

s. Schutz digitaler Infrastrukturen und Kommunikation international zum Durchbruch verhelfen: Obwohl die Geltung des Völkerrechts im Kontext von digitalen Infrastrukturen und persönlicher Kommunikation auf allen internationalen Regelungsebenen anerkannt wird, läuft die seit den 1980er Jahren auf UN-Ebene erhobene Forderung, militärische und geheimdienstliche Aktivitäten in der zivilgesellschaftlichen digitalen Infrastruktur zu ächten, derzeit weitgehend ins Leere. Vor dem Hintergrund zunehmender Bedrohungslagen mit potentiell schwersten Folgen im Fall einer militärischen Konfrontation ist eine Politik der Abschreckung, auch angesichts der Zuordnungs- und Abgrenzungsprobleme von IT-Angriffen („Attribution"), von vornherein zum Scheitern verurteilt. Die Bundesregierung muss sich daher sehr viel stärker als bisher auf internationaler Ebene für einen Verhaltenskodex einsetzen, der eine Gefährdung ziviler (Netz-)Infrastrukturen durch digitale Angriffskapazitäten ausschließt. In einem Multi-Stakeholder-Prozess müssen neue, konkretisierende Regelungen und Vereinbarungen zum Schutz digitaler Infrastrukturen und privater Kommunikation erarbeitet werden.

t. Whistleblowerschutz stärken: Missstände und rechtswidrige Vorgänge in Behörden werden oft erst durch Hinweise von Mitarbeiterinnen und Mitarbeitern bekannt. Gerade bei IT-Sicherheitslücken besteht ein großes öffentliches Interesse an diesen Informationen. Hinweisgeberinnen und Hinweisgeber benötigen einen verbesserten gesetzlichen, arbeits- und dienstrechtlichen Diskriminierungsschutz, um sich unter bestimmten Voraussetzungen straf- und sanktionsfrei an eine außerbetriebliche Stelle, andere zuständige Behörden oder die Öffentlichkeit wenden zu können.

Berlin, den 20. März 2018

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion